Cyberterrorism: The Threat of Virtual Warfare

Summer Olmstead and Dr. Ambareen Siraj
Tennessee Technological University

Cyberterrorism is a threat that has only surfaced worldwide in the past decade—and evidence shows that it is here to stay. With the resourcefulness of terrorists and their adaptability to ever-changing society and technology, it is a form of warfare that needs to be recognized, re-evaluated, and responded to. This article discusses cyberterrorism by exploring its definition; how its attacks on business and government entities know no boundaries; U.S. and international response; current laws; and security engineering design guidelines.

"... cyberspace is real. And so are the risks that come with it." [1]
President Barack Obama, 29 May 2009

Advances in computing technology, along with changes in society, propagated the movement of computers from secret laboratories to the average American household. The more we embrace cybertechnology, the more potential it has for being used against us. Our technical dependence is narrowing the gap between the physical world and the virtual world that surrounds us.

According to the FBI:

> ... terrorism includes the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. [2]

Cyberterrorism is an extension of terrorism, and is a result of the resourcefulness of terrorists and their adaptability to ever-changing society and technology. It is further defined as:

> The premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents. [3]

Cyberterrorism allows terrorists to focus their attacks through virtual warfare from anywhere in the world, at a low cost, with a high level of anonymity, and with no time or space restrictions [4]. Today, cyberterrorism includes a limitless range of crimes, such as defacing Web sites; stealing sensitive information; creating worms, Trojan horses, and viruses; and attacking infrastructures. It can arise from individuals, groups, organizations, nation-states, or countries.

The selection of tools and technologies that a cyberterrorist can utilize include malicious code, hacking, cryptography, and steganography [4]: malicious code or other hacking techniques to get access to systems, and cryptography and steganography for secret communication. Sometimes the public becomes a secondary victim when confidential information (e.g., passwords, social security numbers, credit card numbers, etc.) is stolen and used to aid virtual and real-world terrorist efforts.

"Web site defacement is the most common and extreme visual display of cyberterrorism ... although the aftermath may not always be violent, it does serve the purpose of intimidation ..."

And, of course, the future of cyberterrorism is still being determined by the actions that are being taken now, and will be taken in the near future.

The History of Cyberterrorism

Cyberterrorism has a short history: Only in the past decade have cybersecurity threats surfaced worldwide. Obvious targets of cyberterrorism consist of critical infrastructures—including transportation, electric power grids, oil and gas distribution, telecommunications, air traffic, and financial institutions.

In February 2000, a distributed denial of service (DDoS) attack was launched on popular Internet sites Yahoo, Amazon, eBay, CNN, eTrade, ZDNet, and Datek. Millions of people were unable to access services provided by these companies, resulting in monetary loss and a decline in the sense of security previously offered by these top-tier Web sites [5].

While the focus the following year became physical terrorism (9/11), an incident involving China and the U.S. in April 2001—the collision between an American surveillance plane and a Chinese fighter aircraft—was the likely culprit that initiated a series of cyberattacks and Web site defacements between the two countries [6].

Web site defacement is the most common and extreme visual display of cyberterrorism. It is a form of cyberterrorism because, although the aftermath may not always be violent, it does serve the purpose of intimidation with a political and/or social agenda. Politically motivated Web site defacement has occurred frequently in the past and present. Korean University students defaced Japanese Web sites to protest the content of Japanese textbooks [7]. In protest of the Japanese Prime Minister's visit to the Yasukuni Shrine, pro-Chinese hackers defaced Japanese Web sites. Additionally, the Pakistan-India conflict and the Israel-Palestine conflict both involved Web site defacements [6]. In 2003, Romanian hackers attacked the National Science Foundation's Amundsen-Scott South Pole Station [8]. In 2007, there were several cyberattacks on Estonia, mostly DDoS attacks on police, media, financial, and government Web sites; Estonia claimed that Russia was hacking into their systems. In August 2008, the Georgia-Russia con-

flict continued the pattern of Web site defacements between adversarial nations—both countries' Web sites were defaced during the period of tension over South Ossetia [9].

In early 2009, there was a report [10] that the computer systems that controlled the U.S. power grid were penetrated by foreign threats, likely Russia or China, and evidence of signature software was found. Although no monetary damage was done, the implication is inconceivable. There are many control systems (e.g., SCADA) that exist today with both cyber and physical vulnerabilities and whose unauthorized control/execution/destruction would have far-reaching effects. More recently, July 4, 2009, cyberattacks were launched at the U.S. and South Korea. The U.S. targets of the DDoS attacks included the New York Stock Exchange, Pentagon, Treasury, Secret Service, Department of Transportation, and the White House. There has been speculation that the source of the attacks was from North Korea, but there is currently no solid evidence to confirm this allegation [11]. Countries such as China, Cuba, Iran, Iraq, Libya, North Korea, Russia, Sudan, and Syria are believed to present a greater threat for potential cyberattacks than other nations.

Responding to Cyberterrorism

Cyberterrorism is real, and evidence shows that it is here to stay. While serving as U.S. Attorney General, John Ashcroft said: "One of this nation's most fundamental responsibilities is to protect its citizens, both at home and abroad, from terrorist attacks" [12]. After recognizing cyberterrorism as a genuine security concern, we as a nation should move into a more complex process of responding. In order to win this 21st century electronic war, we should adapt our practices and culture to these drastic changes brought on by the *information age*.

On May 29, 2009, President Obama announced that our digital infrastructure would be treated as a "strategic national asset" and that protecting it would be a national security priority [1]. He also announced the position of the Cybersecurity Coordinator, responsible for overseeing the government's effort to manage, protect against, and respond to cyber incidents.

The development of a new DoD command, U.S. Cyber Command (USCYBERCOM), is another response to cyberthreats by the Obama administration. The goal of the USCYBERCOM is securing our freedom of action in cyberspace [13]. The proposed headquarters would be in Fort Meade, Maryland. The implementation plan was submitted this September to Secretary of Defense Robert Gates. USCYBERCOM is planned to be at full operating capacity by October 2010.

Another response is the establishment of the Cyberterrorism Defense Analysis Center (CDAC), jointly administered by the DHS, Federal Emergency Management Agency, and Training and Exercise Integration/Training Operations [14]. The goal of CDAC is to provide comprehensive cyberterrorism training to technical personnel in critical-need infrastructures.

One method of direct response to cyberterrorism is the establishment of laws addressing cybersecurity. The U.S. government addresses threats to national cybersecurity with the Cyber Security Enhancement Act of 2002, H.R. 3482. This amendment of the Homeland Security Act calls for toughening the authority of the federal government in securing our nation's infrastructures and computer systems. It gives Internet service providers shelter from customer litigation after reporting a customer's suspicious activities and allows more extensive sentencing of cyber criminals, including up to 20 years imprisonment for harmful acts and life imprisonment for life-taking acts [4].

"Cyberterrorism is a global problem and as such requires global attention with initiatives to punish and deter cyberterrorists worldwide."

Because cyberspace is borderless, attacks can originate from anywhere in the world and are not limited by physical boundaries. Cyberterrorism is a global problem and as such requires global attention with initiatives to punish and deter cyberterrorists worldwide. International responses to cyberterrorism include Singapore's Computer Misuse (Amendment) Act of 2003, Pakistan's Prevention of Electronic Crimes Ordinance of 2008, and India's Information Technology (Amendment) Act of 2008. Anyone can fall victim, either by being the target of an attack, or by being an involuntary medium (such as with botnet zombies, a network of computers controlled by malicious code). A sophisticated botnet attack can come from numerous countries at the same time. Therefore, information, intelligence sharing, and cooperation between allied countries are all the more essential to counter cyberterrorism. An example is the International Multilateral Partnership Against Cyber Threats, a coalition of 26 countries with the mission to empower the global community with the capacity to combat cyberterrorism [15].

Cyberterrorism is a complex problem that calls for a comprehensive Defense-in-Depth strategy with particular points of emphasis on prediction (proactive analysis of malicious activities to understand intent, nature, and impact for contingency planning); prevention (securing an environment to avoid penetration); deterrence (applying protection mechanisms to hurdle intruder efforts and thus causing delays in achieving a malicious goal); detection (ensuring visibility of suspicious activities); and response and recovery (reacting to security incidents by eradication, interdiction, and restoration) [16, 17]. These points of emphasis can be implemented by training, awareness, education, preventive security controls, security detection mechanisms, backup and recovery mechanisms, as well as the building of survivable systems.

The future of cyberterrorism can be negatively impacted by increasing the level of difficulty for terrorists to access vulnerabilities and decreasing the surprise and anonymity of attacks. Security engineering can help in this respect—where security is not an afterthought, but carefully dealt with from the beginning of the system life cycle. According to [18], the 10 design guidelines of security engineering are to:

1. Base security decisions on an explicit security policy.
2. Avoid a single point of failure.
3. Fail securely.
4. Balance security and usability.
5. Be aware of the possibility of social engineering.
6. Use redundancy and diversity to reduce risk.
7. Validate all input.
8. Compartmentalize assets.
9. Design for deployment.
10. Design for recoverability.

These guidelines should be part of the DoD software community culture and practice, as they hold the responsibility for development and maintenance of government software systems, in turn being the key target of cyberterrorists. Interweaving security engineering practices with designing, developing and testing systems, and management of cyberterrorism by proper

Software Defense Application

Cyberterrorism is a form of 21st century warfare that needs to be examined, especially in the DoD software community culture, where practitioners hold the responsibility for development and maintenance of government software systems, in turn being the key target of cyberterrorists. This article looks at cyberterrorism by examining its definition, history, sources, current laws, and government responses, and provides security engineering design guidelines especially useful in the DoD.

risk assessment and contingency planning, can only strengthen our nation's defense for today and tomorrow.

Counter-cyberterrorism is essential. It can take the form of an average citizen who uses strong passwords for electronic accounts, a technically high-skilled *white hat* who knows how to disable malicious code, or a government official who ensures that security policies and practices are in place and properly followed. Even if cyberterrorism cannot be completely eliminated, it can mostly be prepared for, prevented to some extent, and its damage contained.

In conclusion, the absolute defense against terrorism and cyberterrorism is extremely difficult. Although cyberterrorism is currently prevailing mostly in the virtual world, technological advancements make its ability to disrupt our physical world just as possible—if not even more likely. Constantly changing technology advances our quality of life but also changes the landscape of 21st century warfare. Cyberterrorism demonstrates the ability of terrorism to adapt to the modern world and shows why it is important to continue recognizing this threat by minimizing opportunities and devoting resources to its prevention.◆

References

1. "Remarks by U.S. President Barack Obama on Securing the Nation's Cyber Infrastructure." *BBC News*. 29 May 2009 <http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/29_05_09_cyber.pdf>.
2. Code of Federal Regulations, 28 C.F.R. Section 0.85 (July 2001): 51.
3. Pollitt, Mark M. "CYBERTERRORISM – Fact or Fancy." Georgetown University. Department of Computer Science. 10 June 2009 <www.cs.georgetown.edu/~denning/infosec/pollitt.html>.
4. Kim, Jeongtae, Soyoung Park, and Tchanghee Hyun. *An Inquiry into International Countermeasures Against Cyberterrorism*. Proc. of the 7th International Conference on Advanced Communication Technology. Gangwon-Do, Korea, 2005: 432-35.
5. Biegel, Stuart. *Beyond Our Control? Controlling the Limits of Our Legal System in the Age of Cyberspace*. New York: The MIT Press, 2003.
6. Keegan, Christopher. "Cyber-Terrorism Risk." *Financial Executive* 18.8 (Nov. 2002): 35-37.
7. Bronk, Chris. "Hacking the Nation-State: Security, Information Technology and Policies of Assurance." *Information Security Journal: A Global Perspective* 17.3 (2008): 132-142.
8. "The Case of the Hacked South Pole." *Federal Bureau of Investigation Headline Archives*. 14 Apr. 2009 <www.fbi.gov/page2/july03/071803backsp.htm>.
9. Cluley, Graham. "Conflict Between Russia and Georgia Turns to Cyber Warfare." Weblog post. *Sophos*. 12 Aug. 2008 <www.sophos.com/blogs/gc/g/2008/08/12/conflict-between-russia-and-georgia-turns-to-cyber-warfare/>.
10. Ghosh, Bobby. "How Vulnerable is the Power Grid?" *Time*. 15 Apr. 2009 <www.time.com/time/printout/0,8816,1891562,00.html>.
11. Baldor, Lolita C. "White House Among Targets of Sweeping Cyber Attack." *Associated Press*. 8 July 2009 <http://abcnews.go.com/Technology/wireStory?id=8029944>.
12. Ashcroft, John. "Statement of Attorney General John Ashcroft ... on U.S. Federal Efforts to Combat Terrorism." Joint Hearing on Federal Efforts to Combat Terrorism." *The Avalon Project*. Yale Law School Lillian Goldman Law Library. 3 Apr. 2009 <http://avalon.law.yale.edu/21st_century/t_0016.asp>.
13. Gates, Robert M. U.S. Secretary of Defense. "Establishment of a Subordinate Unified Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations." Memorandum. 23 June 2009 <www.publicintelligence.net/?p=1010>.
14. Cyberterrorism Defense Initiative. 1 Sept. 2009 <www.cyberterrorismcenter.org>.
15. International Multilateral Partnership Against Cyber Threats <www.impact-alliance.org>.
16. "Defense-in-Depth Strategy Optimizes Security" *Intel Information Technology*. 1 Sept. 2009 <http://ipip.intel.com/go/3941/defense-in-depth-strategy-optimizes-security/>.
17. Siraj, Ambareen. Lecture Notes CSC 6575. Dept. of Computer Science. Tennessee Tech University. 2009.
18. Sommerville, Ian. *Software Engineering*. 8th ed. Essex, England: Addison-Wesley, 2007. 731-737.

Additional Reading

1. Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Indianapolis: Wiley Publishing, Inc., 2008.
2. Viega, John, and Gary McGraw. *Building Secure Software: How to Avoid Security Problems the Right Way*. New York: Addison-Wesley, 2001.

About the Authors

Summer Olmstead is completing her bachelor's degree in computer science at Tennessee Tech University. Her interests lie in the areas of information assurance and security.

Tennessee Tech University
P.O. Box 14734
Cookeville, TN 38505
Phone: (931) 252-7025
E-mail: smolmstead21@tntech.edu

Ambareen Siraj, Ph.D., is an assistant professor of computer science at Tennessee Tech University. She obtained her doctorate in computer science from Mississippi State University. Her research interests include information assurance and security, artificial intelligence, and software engineering.

Department of Computer Science
Tennessee Tech University
Cookeville, TN 38505
Phone: (931) 528-6081
E-mail: asiraj@tntech.edu